APPENDIX

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE CLAIMS:

Please cancel claims 14-16.

The claims are amended as follows:

3. A data capture device as claimed in~~ either~~ claim 1~~ or claim 2~~ wherein a data capture device is a digital video camera.

4. A data capture device as claimed in~~ any one of~~ claims 1~~ to 3~~ which adds a watermark to the image captured by the data capture device.

5. A data capture device as claimed in~~ either~~ claim 3~~ or claim 4~~ which includes the ability to detect motion.

6. A data capture device as claimed in~~ any one of~~ claims 3~~ to 5~~ which includes means to distinguish over false detection of motion.

7. A data capture device as claimed in~~ any one of~~ claims 3~~ to 6~~ which includes means to track objects record the path of movement through the field of view.

8. A data capture device as claimed in~~ any one of~~ claims 3~~ to 7~~ which includes infra-red motion detection.

9. A data capture device as claimed in~~ any one of~~ claims 3~~ to 8~~ which includes a wide angled lens and an image capture assembly fitted internally at approximately 45 degrees.

10. A data capture device as claimed in~~ any one of~~ claims 3 ~~to 9~~characterised in that the camera can be fixed into position by pushing and rotating the camera until it locks onto a mounting bracket which has electrical connections that connect to the camera once mounted.

13. A monitoring system which includes a data capture device as claimed in~~ any one of~~ claims 1 ~~to 11~~.

IMPROVEMENTS IN OR RELATING TO CONTROL AND/OR MONITORING SYSTEMS

This invention relates to improvements in or relating to control and/or monitoring systems.

Reference around the specification should be made to the present invention in relation to security systems which are in fact control and/or monitoring systems.

BACKGROUND ART

An increasing number of security systems arc bcing installed world-wide. Further, existing security systems are continually being upgraded as technology becomes smarter, more monitoring/control devices are available, and the desirc for increased security increases.

Some representative systems are described in EP-A-0689357 (Harris Corp) and US-A-5689442 (Mocn Jcrry Mctal)

Most complexes into which the systems are installcd have existing communications networks. These networks all have various constraints which may include cabling, data transmission, proccssing and storage.

Each time a peripheral devicc for a security systcm is added to the communications network, a number of tasks maybe required to cnable this to happen, These may include

- Adding additional softwarc to the server of the communications network to process/translate the data entering the network from the peripheral.
- Adding extra cabling to connect the periphcral to thc local area network or dirctly to thc scrvcr.

- Upgrading the cabling of the local area network to accommodate increased rates of data transmission.

- Increasing the memory of the server in order to store additional data.

- Increasing the processing power of the server to handle the extra data.

To implement any of the above is expensive and time consuming. Further, implementation can lead to worker's downtime and possible security risks as the system is being taken offline to accommodate the changes being made.

Another problem associated with security systems is that the persons monitoring the system are exposed to a considerable volume of information. This can include a multiplicity of screens which must continually be monitored effectively. What can occur is an information overload when the person watching cannot continually assimilate all of the information in a manner that facilitates an efficient or effective monitoring function. Thus, it is possible that "alarm" and "unusual" situations can appear on the screens but not be seen or be acted upon as quickly as desired.

Another problem with security systems that utilise existing communications architecture is that the system may become inoperative, for example the server may "crash".

Thus, the security system can be dependant upon an unreliable communications network and disabled along with it. In some situations, it maybe that parties wishing to breach security will target this network.